Chapter 1: Network Security Terminology

In This Chapter

- **Introduction to security terminology**
- **Identifying types of attacks**
- **Looking at security devices**
- **Mitigating security threats**

One of the most important skills to have if you are going to support networked systems or systems connected to the Internet is the ability of securing systems and networks. In order to be successful as a network professional today, you need to have a solid understanding of network security and ways to protect the network.

I remember when a close friend of mine had his Web site totally replaced by a hacker. My friend's Web site files were replaced with inappropriate content, and he wondered how on Earth someone had hacked his server. It seems amazing now, but back then (circa 1994) a lot of companies did not use firewalls because they were not aware of the risks involved in having a computer connected directly to the Internet. Back then, people thought, "I have a password on the administrator account, so I am secure."

In this chapter, you find out about the basic concepts and terminology related to information system security and network security. Be sure to read this chapter carefully, and make sure you understand the topics, as you will be tested on basic security concepts with the CCENT certification exam. Have fun with this topic area — security is a very exciting field!

COPYRIGHTED MATERIAL

Quick Assessment

1. (True/False). A packet-filtering firewall checks the state of the conversation.
2. A _____ is responsible for creating a secure tunnel over an unsecure network.
3. The term used for controlling who is allowed to access a resource is _____.
4. (True/False). A dictionary attack calculates all potential passwords.
5. A _____ virus is a self-replicating virus.

Answers

1 *False*. See "Firewalls."

2 *VPN*. Review "Virtual Private Networks."

3 *Authorization*. Check out "Authorization."

4 *False*. Peruse "Password attacks."

5 *Worm*. Take a look at "Worm."

Introduction to Security Terminology

Let me start the discussion by going over some basic security concepts and terminology. The CCENT certification exam expects you to have some background in security best practices, so this chapter is designed to expose the concepts to you. The next chapter looks at specific steps you need to take to secure your Cisco devices.

Authentication

Authentication is the process of proving one's identity to the network environment. Typically, authentication involves typing a username and password on a system, and it is then verified against an account database before you are granted access. There are different methods you can use to authenticate to a system or network — you can supply a valid username and password or maybe even use biometrics to be authenticated. *Biometrics* is the concept of using a unique physical characteristic of yourself to authenticate to the system, such as a fingerprint, a retina scan, or voice recognition to prove your identity.

Consider these three different forms of authentication, known as *authentication factors,* and their uses:

- **Something you have:** Dependent on the user having an object in her possession to prove who she is. An example of this authentication is possession of an ID card or door key.
- **Something you know:** Dependent on the user knowing a piece of information to validate who he is. Examples of this are knowledge of a password, pass code, or even a PIN (personal identification number).
- **Something you are:** Dependent on you proving your identity by something you are, such as a fingerprint or retina scan — so biometrics falls into this authentication factor.

Most authentication systems use a *two-form* authentication factor, where two of the three factors mentioned here are used. For example, it is not enough to have the ATM card in your possession to use it — you must know the PIN for that card as well.

Smart card

A popular authentication device used today in networking environments is a smart card, which is a small, ATM card–like device that contains your account information. You insert the smart card into a smart card reader that is connected to a computer, and then you enter the PIN associated with the smart card. This is an example of securing an environment by requiring the user to not only have the card, but also know the PIN — an example of two-form authentication.

Using strong passwords

A number of years ago, I had a coworker who was always trying to get me to guess his passwords. He thought I had some magical trick or program that was cracking them, but all I was doing was guessing his passwords. I remember one time he changed it, and I could not guess it — until one night when we were at a social function for work and all he talked about was the Flyers hockey team. I remember sitting there thinking, "I bet that is his password." Sure enough, the next day at work, I tried `flyers` as his password, and it worked. Now the lesson here is that he should have at least mixed the case of the word *flyers* to make something like `flYeRs`, or even better, thrown a symbol in there by replacing the *s* with a *$*. I would have had a much harder time trying to guess his password if he had used `flYeR$` instead. This is an example of a strong password.

Strong passwords

It is really hard to talk about authentication without talking about ensuring your usage of strong passwords on systems and devices. A *strong password* is a password that is very difficult for hackers to guess or crack because it contains a mix of uppercase and lowercase characters, a mix of numbers and letters, and is a minimum of six characters long.

Authorization

After someone is authenticated to a system or device, he is then granted or denied access to resources such as files and printers, or given limited privileges to a device. *Authorization* is the process of giving a person permission to access a resource or a device.

Do not confuse authentication and authorization: You must be first *authenticated* to the network; then, after authentication, you can access the resources and perform the tasks that you have been *authorized* for.

An example of authorization in the networking world is choosing to authorize a system on the network (meaning we allow it to connect to the network through a port on the switch) by its MAC address. In high-security environments, this is very popular, and in the Cisco world, this is known as *port security*.

Vulnerability

Vulnerability is the term we use for a weakness in a system or device. The vulnerability is created accidentally by the manufacturer and is typically the result of a code mistake in the software or firmware.

Hackers find out about vulnerabilities in the software and hardware devices we use by purposely testing the limitations of the device or software. Once they discover the vulnerability, they work on figuring out how they can exploit it.

Exploit

An *exploit* takes advantage of a weakness, or vulnerability, in a piece of software or a device. For example, years ago it was found that most Web servers were vulnerable to attack because the Web server did not verify the file being requested in a URL. Hackers exploited this by starting to send commands in a URL that would navigate the folder structure of the Web server and call for files other than normal Web pages. This is known as *folder traversing,* and it was a popular exploit on Web servers.

What about CIA?

When working in the security field, you will most likely run into the terms *confidentiality, integrity, availability* (CIA). These are the fundamental goals of security, and ultimately, every security control that we put in place satisfies one of the elements of CIA.

Confidentiality

Confidentiality is the concept of keeping information secret. In order to implement confidentiality, you may look to securing data with permissions, but you also have to look at encrypting the information that is stored on disk or travels across the network.

Integrity

Integrity is the veracity of the data. *Data integrity* is about ensuring that when you receive information, it is the information that was actually sent and not something that was modified in transit. *Hashing* is one of the popular methods of ensuring data integrity. With hashing, the data sender runs the data through a mathematical algorithm (known as a *hashing algorithm*), and an answer is created. When the recipient receives the information, she runs the data on the same algorithm to see if she gets the same mathematical answer. If the same answer is calculated, she knows that the data has not been altered in transit.

Availability

Availability is the concept that the data stored on the network is always accessible to the people who want the data — the people who are authorized to access it, that is. As security professionals, we need to ensure the availability

of the data, and there are a number of ways to ensure availability. For example, you can do backups, use RAID volumes for storing your data, and implement high-availability solutions such as *clustering technologies* (multiple servers running the same application, or service, so if one server fails the request for the service is sent to the second server).

Identifying Types of Attacks

Now that you are familiar with some basic network security terms, let's talk about some popular attacks against businesses today. These attacks may sometimes seem far-fetched, but in reality, they happen every day! This section outlines some of the most popular types of attacks that can happen in today's networking environments.

For the CCENT certification exam, it is critical that you are familiar with the different types of attacks covered in this section. You are sure to get a few questions about types of attacks.

To me, a hacker is someone with the technical expertise to bypass the security of a network or a system. A hacker knows how to use features of a piece of software or hardware to gain access to restricted areas of a network and then use those features against you and your system. For example, an e-commerce Web site connects to a product database behind the scenes so that you can get a list of products when you visit the site. A hacker knows how to input data into the site to manipulate the database server into executing the code that the hacker wants to execute — and this happens because the hacker understands the technologies used behind the scenes.

There are two major types of hackers:

- **Black-hat hackers:** Break into a system or network for malicious reasons or for personal gain. The black-hat hacker could be looking for financial gain, bragging rights, or revenge.
- **White-hat hackers:** Try to hack into software or hardware in order to understand how to protect others from black-hat hackers. These are the good guys.

Hackers use a number of different types of attacks to hack into a network, device, or a system. Sometimes an attack lays the groundwork for a future or different type of attack: That is, the initial attack does not seem all that dangerous, but it is used in the future to gain unauthorized access.

Social engineering attacks

A *social engineering attack* occurs when a hacker tries to obtain information or gain access to a system through social contact with a user. Typically, the hacker poses as someone else and tries to trick a user into divulging personal or corporate information that allows the hacker access to a system or network.

For example, a hacker calls your company's phone number, listed in the phone book, and poses as a technical support person for your company. He tells the user who answers the phone that a new application has been deployed on the network, and for the application to work, the user's password must be reset. After the password is reset to what the hacker wants, he might "verify" with the user the credential that the user uses. A user who is not educated on social engineering might divulge important information without thinking that the caller might have malicious intent.

A social engineering attack is an attack where a hacker tries to trick a user or administrator into divulging sensitive information through social contact. After the sensitive information is obtained, the hacker can then use that information to compromise the system or network.

This example might sound unrealistic, but it happens all the time. If you work for a small company, you might not experience a social engineering attack. In a large corporate environment, though, it is extremely possible that a social engineering attack would be successful if the company does not educate its users. A large company usually stations the IT staff or management at the head office, but employees in most branch locations have never talked to IT management. The branch employees would not recognize the voices of the IT folks, so a hacker could impersonate someone from the head office — and the user at the branch office would never know the difference.

There are a number of popular social engineering attack scenarios — and network administrators are just as likely to be social engineering victims as "regular" employees, so they need to be aware. Here are some popular social engineering attack scenarios:

- **Hacker impersonates an IT administrator.** The hacker calls or e-mails an employee and pretends to be the network administrator. The hacker tricks the employee into divulging a password or even resetting the password.
- **Hacker impersonates a user.** The hacker calls or e-mails the network administrator and pretends to be a user who forgot her password, asking the administrator to reset her password for her.
- **Hacker e-mails a program to network users.** The hacker typically e-mails all the users on a network, telling them about a security bug in the OS. He advises users to run the `update.exe` file attached to the e-mail. In this example, `update.exe` is the attack file — it opens the computer up so that the hacker can access the computer.

When you are working as a network professional, educate your users never to run a program that has been e-mailed to them. Most software vendors, such as Microsoft, state that they will never e-mail a program to a person: Instead, they will e-mail a URL, but it is up to the person to go to the URL and download the update. A great book to find out more on the process a hacker employs to compromise a system is Kevin Beaver's *Hacking For Dummies,* 3rd edition (Wiley).

Network-based attacks

A *network-based attack* uses networking technologies or protocols to perform the attack, and they are some of the most popular types of attacks today. The following explains the terminology associated with seven important network-based attacks.

Ensure that you are familiar with the different types of network-based attacks for the CCENT certification exam.

Password attacks

A *password attack* involves the hacker trying to figure out the passwords for different accounts on a system, or a password that guards a device. The three major types of password attacks are dictionary attack, hybrid attack, and brute force attack.

With a *dictionary attack*, hackers use a program in conjunction with two text files to automatically try a number of passwords.

- One text file contains the most popular user accounts — such as administrator, admin, and root — found on networks. This file is termed the user account text file.
- The second text file contains a list of all the words in the English dictionary, and then some. Hackers can also obtain dictionary files for different languages. This file is termed the dictionary text file or password list file.

The dictionary attack program then tries to log in with every user account in the user account text file with every word in the dictionary text file, attempting to determine the password for the user account.

To protect against a dictionary attack, be sure to use strong passwords that mix letters, numbers, and symbols. This prevents the passwords from being found in the dictionary. Also, passwords are normally case sensitive, so be sure to use a mix of both lowercase and uppercase characters. Mixing the case of a password means a hacker not only has to guess the password but also the combination of uppercase and lowercase characters.

Also note that because there are dictionary files for different languages you should not use words found in *any* dictionary. This means avoiding not only English words, but also French, German, Hebrew . . . even Klingon!

A second type of password attack is known as a hybrid password attack. A *hybrid password attack* is like a dictionary attack in the sense it uses a dictionary file, but it also tries variations of the password by placing numbers on the end of the word and sometimes replacing popular characters. For example, after the hybrid attack program tries all the passwords in the dictionary file, it may then try them again by replacing any letter *a* with @ in the words.

Hackers can also perform a *brute force attack*. With a brute force attack, instead of trying to use words from a dictionary file, the hacker uses a program that tries to figure out your password by mathematically calculating all potential passwords with a certain length and set of characters. Figure 1-1 shows a popular password-cracking tool known as LC4. Tools like this are great for network administrators to audit how strong their users' passwords are.

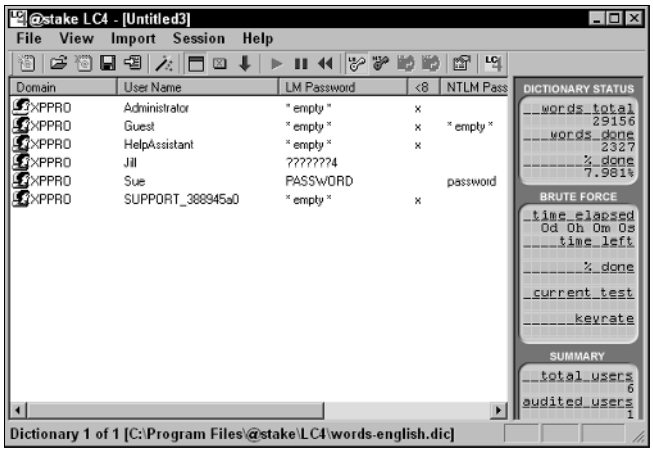

Figure 1-1: Cracking passwords with LC4.

To protect against dictionary attacks, we use strong passwords, but to protect against a brute force password attack, we must implement an *account lockout policy,* where after three bad logon attempts, the account is locked and cannot be used.

If you have configured an account lockout policy to protect your account database, understand that only works if the hacker is connected to your network and attempting to hack into live systems (known as an *online attack*). If the hacker can get a copy of your account database, or hashed passwords in a configuration file, and take that away with him (known as an *offline attack*) then there is no protection against the brute force attack.

Denial of service

Another popular network attack is a *denial of service (DoS)* attack, which can come in many forms and is designed to cause a system or network device to be so busy that it cannot service a real request from a client, essentially overloading the system or device and shutting it down.

For example, say you have an e-mail server and a hacker attacks the e-mail server by flooding the server with e-mail messages, causing it to be so busy that it cannot send any more e-mails. You have been denied the service that the system was created for.

There are a number of different types of DoS attacks that have come out over the years, including the following:

- **Ping of death:** The hacker continuously pings your system with oversized packets causing your system to crash.
- **SYN flood:** The hacker performs a partial three-way handshake with each port on the system. This uses up memory on your system and eventually crashes the system. The hacker accomplishes this by sending a SYN message to a number of different ports, but when your system replies with an ACK/SYN, the hacker does not complete the process with an ACK. As a result your system holds that partial connection in memory, waiting for the ACK. For more on the three-way handshake, SYN, and ACK, see Book I, Chapter 4.

To protect against denial of service attacks, you need to have a *firewall* (a piece of software or a hardware device that prevents someone from entering your system or network) installed, and you should also keep your systems and devices patched (apply any updates and security fixes).

Spoofing

Spoofing is a type of attack in which a hacker modifies the source address of a frame or packet. There are three major types of spoofing:

- **MAC spoofing:** The hacker alters the source MAC address of the frame.
- **IP spoofing:** The hacker alters the source IP address in a packet.
- **E-mail spoofing:** The hacker alters the source e-mail address to make the e-mail look like it came from someone other than the hacker.

An example of a spoof attack is the *smurf attack*, which is a combination of a denial of service *and* spoofing. Here is how it works:

1. The hacker pings a large number of systems but modifies the source address of the packet so that the ping request looks like it is coming from a different system.

2. All systems that are pinged reply to the modified source address — an unsuspecting victim.
3. The victim's system (most likely a server) receives so many replies to the ping request that it is overwhelmed with traffic, causing it to be unable to answer any other request from the network.

To protect against spoof attacks, you can implement encryption and authentication services on the network.

Eavesdropping attack

An *eavesdropping attack* occurs when a hacker uses some sort of packet sniffer program to see all the traffic on the network. Hackers use *packet sniffers* to find out login passwords or to monitor activities. Figure 1-2 shows Microsoft Network Monitor, a program that monitors network traffic by displaying the contents of the packets.

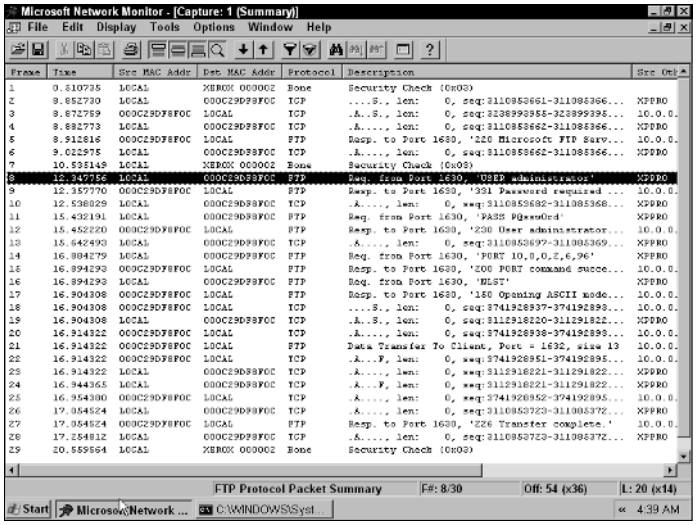
Microsoft Network Monitor - [Capture: 1 (Summary)]
File Edit Display Tools Options Window Help
Frame Time Src MAC Addr Dst MAC Addr Protocol Description Src Oth
1 0.810735 LOCAL XEROX 000002 Bone Security Check (0x08)
2 8.652730 LOCAL 000C29D98F0C TCP ....S., len: 0, seq:3110853661-311085366... XPPRO
3 8.672759 000C29D98F0C LOCAL TCP .A..S., len: 0, seq:3238993955-323899395... 10.0.0.
4 8.882773 LOCAL 000C29D98F0C TCP .A...., len: 0, seq:3110853662-311085366... XPPRO
5 8.912816 000C29D98F0C LOCAL FTP Resp. to Port 1630, '220 Microsoft FTP Serv... 10.0.0.
6 9.022975 LOCAL 000C29D98F0C TCP .A...., len: 0, seq:3110853662-311085366... XPPRO
7 10.538149 LOCAL XEROX 000002 Bone Security Check (0x08)
8 12.347756 LOCAL 000C29D98F0C FTP Req. from Port 1630, 'USER administrator' XPPRO
9 12.357770 000C29D98F0C LOCAL FTP Resp. to Port 1630, '331 Password required ... 10.0.0.
10 12.538829 LOCAL 000C29D98F0C TCP .A...., len: 0, seq:3110853682-311085368... XPPRO
11 15.432191 LOCAL 000C29D98F0C FTP Req. from Port 1630, 'PASS P@ssw0rd' XPPRO
12 15.452220 000C29D98F0C LOCAL FTP Resp. to Port 1630, '230 User administrator... 10.0.0.
13 15.642493 LOCAL 000C29D98F0C TCP .A...., len: 0, seq:3110852697-311085369... XPPRO
14 16.894279 LOCAL 000C29D98F0C FTP Req. from Port 1630, 'PORT 10,0,0,2,6,96' XPPRO
15 16.894292 000C29D98F0C LOCAL FTP Resp. to Port 1630, '200 PORT command succe... 10.0.0.
16 16.894293 LOCAL 000C29D98F0C FTP Req. from Port 1630, 'NLST' XPPRO
17 16.904308 000C29D98F0C LOCAL FTP Resp. to Port 1630, '150 Opening ASCII mode... 10.0.0.
18 16.904308 000C29D98F0C LOCAL TCP ....S., len: 0, seq:3741926937-374192893... 10.0.0.
19 16.904308 LOCAL 000C29D98F0C TCP .A..S., len: 0, seq:3112918220-311291822... XPPRO
20 16.914322 000C29D98F0C LOCAL TCP .A...., len: 0, seq:3741926938-374192893... 10.0.0.
21 16.914322 000C29D98F0C LOCAL FTP Data Transfer To Client, Port = 1632, wire 13 10.0.0.
22 16.914322 000C29D98F0C LOCAL TCP .A...F, len: 0, seq:3741926951-374192895... 10.0.0.
23 16.914322 LOCAL 000C29D98F0C TCP .A...., len: 0, seq:3112918221-311291822... XPPRO
24 16.944365 LOCAL 000C29D98F0C TCP .A...F, len: 0, seq:3112918221-311291822... XPPRO
25 16.954380 000C29D98F0C LOCAL TCP .A...., len: 0, seq:3741926952-374192895... 10.0.0.
26 17.054524 LOCAL 000C29D98F0C TCP .A...., len: 0, seq:3110853723-311085372... XPPRO
27 17.054524 000C29D98F0C LOCAL FTP Resp. to Port 1630, '226 Transfer complete.' 10.0.0.
28 17.254812 LOCAL 000C29D98F0C TCP .A...., len: 0, seq:3110853723-311085372... XPPRO
29 20.559564 LOCAL XEROX 000002 Bone Security Check (0x08)
FTP Protocol Packet Summary F#: 8/30 Off: 54 (x36) L: 20 (x14)
Start Microsoft Network ... C:\WINDOWS\Syst... 4:39 AM

Figure 1-2: Using Network Monitor to analyze FTP logon traffic.

Notice in Figure 1-2 that the highlighted packet (frame 8) shows someone logging on with a username of `administrator`; in frame 11, you can see that this user has typed the password `P@ssw0rd`. In this example, the hacker now has the username and password of a network account by eavesdropping on the conversation!

To protect against eavesdrop attacks, you need encrypt network traffic and physically control who can connect to your network.

Man-in-the-middle

A *man-in-the-middle attack* involves the hacker intercepting the data in transit, potentially modifying the data, and then forwarding the information on to the intended recipient. Note that the intended recipient receives the information, but the hacker sees the information as well.

Man-in-the-middle attacks are popular with wireless networks at coffee shops today. The hacker poisons the ARP cache of the wireless clients so that they forward all the traffic to the hacker's system first, who then forwards the information onto the Internet. The clients are still surfing the Internet, but what they do not realize is that they are passing through the hacker's laptop first. (And the hacker is typically capturing all the traffic with a packet sniffer in hopes of capturing user passwords.)

To protect against man-in-the-middle attacks, you need to restrict access to the network and implement encryption and authentication services on the network.

Session hijacking

A *session hijack* is similar to a man-in-the-middle attack, but instead of the hacker intercepting the data, altering it, and sending it to whomever it was destined, the hacker simply hijacks the conversation by disconnecting one of the participants off the network (usually via a denial of service attack) and then impersonates that person within the conversation. The other party has no idea that he or she is communicating with someone other than the original person.

To protect against session hijacking attacks, you need to restrict access to the network and implement encryption and authentication services on the network.

Buffer overflow

A very popular type of attack today is a *buffer overflow attack,* which involves the hacker sending more data to a piece of software than the software expects. The information sent to an application is typically stored in an area of memory known as a *buffer*. When more data than expected is sent to the application, the information is stored in memory beyond the allocated buffer. It has been found that if a hacker can store information beyond the allocated buffer, he can run his own code that typically results in a remote command shell with administrative access. The reason why administrative access is gained is because the code executes in the context of the user account associated with the software that was hacked — normally an administrative account!

To protect against buffer overflow attacks, you need to keep the system, applications, and devices up to date with patches and security fixes.

Software-based attacks

Just like there are a number of different types of network attacks, there are a number of software attacks. As you can likely guess, a *software attack* comes through software that a user runs. The most popular software attacks are mentioned in the sections that follow, and you should be familiar with them for the CCENT certification exam.

SQL injection

A *SQL injection attack* occurs when the hacker sends `Transact SQL` statements (statements that manipulate a database) into an application so that the application will send those statements to the database server to be executed. If the application developer does not validate data inputted into the application, the hacker can modify the data in the underlying database or even manipulate the system.

Viruses

A *virus* is a program that causes harm to your system. Typically, viruses are spread through e-mails and are included in attachments, such as word processing documents and spreadsheets. The virus can do any of a number of things: It can delete files from your system, modify the system configuration, or e-mail all your contacts in your e-mail software. To prevent viruses, install antivirus software and do not open any unexpected file attachments that arrive in your e-mail.

Trojan horse

A *Trojan horse* is a type of virus that a user is typically tricked into running on the system, and when the software runs, it does something totally different from what the user expected it to do. For example, NetBus (an older Trojan horse virus) is an example of a Trojan horse virus sent as a file called `patch.exe`. The user receiving the file — typically through an e-mail — believes the file will fix a security issue. The problem is that `patch.exe` is a Trojan horse, and when that horse starts running, it opens the computer up to allow a hacker to connect to the system.

The hacker then uses a client program, like the one shown in Figure 1-3, to connect to the system and start messing with the computer. The hacker can do things like launch other programs, flip your screen upside down, eject your CD-ROM tray, watch your activity, and modify or delete files!

Worm

A *worm* is a virus that does not need to be activated by someone opening the file. It is *self-replicating,* meaning that it spreads itself from system to system

automatically, infecting each computer. How the virus spreads depends on the virus itself — there have been worm viruses that connect across the network automatically to a vulnerable system and then infect that system. Recently, worm viruses automatically infect a flash drive that is connected to the system so that when you take the drive to the next system, the worm infects that system from the flash drive.

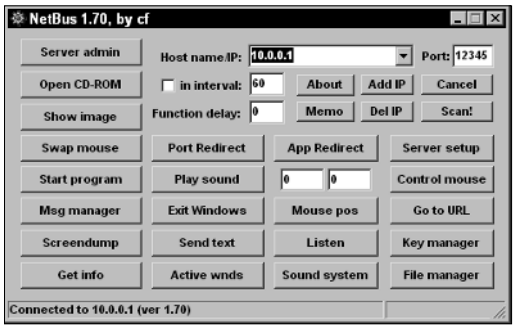

Figure 1-3: Using a Trojan virus known as NetBus to control a user's computer.

Logic bomb

A *logic bomb* is a type of virus or malicious software that was designed to wreak havoc on your system on a certain date and time. The scary thing about logic bombs is that they seem like useful software until the day the programmer decides it will become malicious!

To protect against malicious software such as a virus, Trojan horse, worm, and a logic bomb, you need to use a firewall and keep your virus definitions up-to-date.

Looking at Security Devices

When looking to secure your systems or networks, you can definitely follow best practices such as patching systems or using strong passwords, but realistically, you are going to need to use one or more popular security devices to secure your environment. In this section, I discuss popular security devices you should be familiar with for the CCENT certification exam.

Firewalls

A *firewall* is a piece of software or a device that is designed to control what traffic is allowed to enter or leave the network. Most firewalls control traffic that enters the network by analyzing the header of the packet and looking at the source IP address, destination IP address, and the source and destination port. If the packet trying to enter the network meets certain conditions, such

as the destination port is 80, the packet is then allowed or denied access to the network depending on how the firewall is configured.

There are three major types of firewalls that are popular today:

- **Packet-filtering firewall:** A packet-filtering firewall is limited in the sense that it filters traffic by the fields in the header such as the source and destination IP address and the source and destination port numbers. It is very easy for the hacker to bypass this firewall; she can alter the fields in the header.
- **Stateful packet inspection firewall:** Most firewalls today are stateful packet inspection firewalls, which filter traffic by the fields in the header but also can understand the context of the conversation. For example, a stateful packet inspection firewall knows that before you can send data to a Web site you must have had a three-way handshake with the system. The firewall stores the "state" of the conversation in a state table so it can verify that the packet it is receiving should actually be occurring at this point in time.
- **Application-level firewall:** An application-level firewall has the benefit of not only being able to analyze the fields in the header and being stateful, but it has the added benefit of being able to analyze the application data that is stored in the packet. For example, an application-layer firewall can verify that a three-way handshake has occurred and that the destination port is 80, but it can also verify that the HTTP command in the packet is a `GET` and not a `POST`. These firewalls can limit what features of an application are allowed to be performed.

There are many different ways to implement a firewall solution, and most networks use multiple firewalls to control access to different parts of the network. Figure 1-4 shows a very popular firewall solution that uses two firewalls.

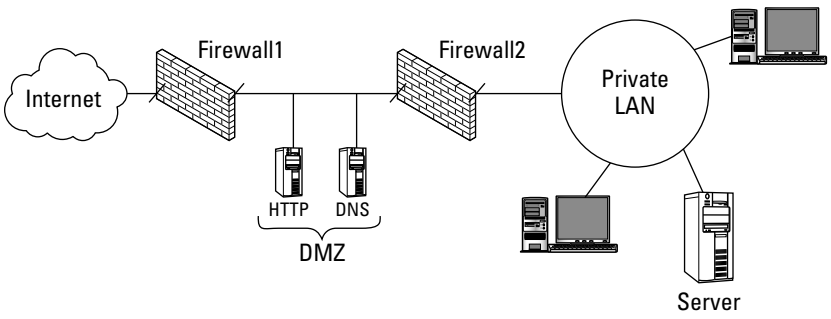

Figure 1-4: Firewalls are used to protect the internal network from unauthorized traffic.

The first firewall (Firewall1 in Figure 1-4) is connected to the Internet and controls what traffic is allowed to pass from the Internet through the firewall. You can see that the first firewall has to allow HTTP traffic and DNS server traffic through the firewall, as there are public HTTP and DNS servers behind the first firewall.

The second firewall (Firewall2 in Figure 1-4) is designed to stop all traffic from passing through that firewall in order to protect the private LAN. The area between the two firewalls is known as a *demilitarized zone* (DMZ) and is designed to allow selected traffic to enter the zone. This firewall solution is known as a *screened-subnet* as any traffic that passes into the DMZ is screened first and ensured it is authorized traffic.

Another very popular firewall solution that relates to Cisco devices is what is known as a *screened-host firewall,* shown in Figure 1-5. It is a topology that has the Internet connected to your router, which will then *filter,* or screen, what packets are allowed to pass through and reach the firewall.

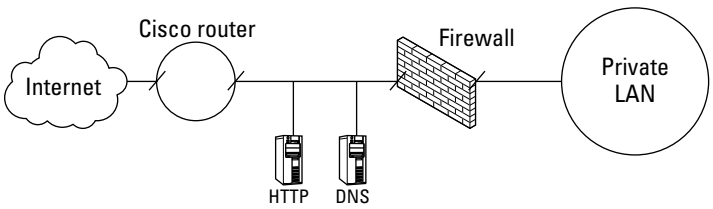

Figure 1-5: A screened-host firewall uses a router to filter which packets reach the firewall.

Cisco routers use *access lists* (a list of rules that determine what packets are allowed to enter or leave the network) to control what traffic is allowed to pass through the router. Access lists are beyond the scope of the CCENT certification but are required knowledge to pass the CCNA certification exam.

Intrusion detection system

An *intrusion detection system* (IDS) is a device or piece of software that monitors activity and identifies any suspicious activity on a network or system. When the IDS identifies the suspicious activity, it logs the activity and may even send notification to the administrator as an alert.

There are two main types of intrusion detection systems:

- **Host-based IDS:** This is typically software installed on the system that monitors activity on that one system. If suspicious activity is found on the system an alert is generated and the administrator is notified.
- **Network-based IDS:** Monitors network traffic and identifies suspicious traffic on the entire network, not just one system! The network-based IDS captures network traffic and then compares that to signatures in the IDS software. This analysis indicates what type of traffic is considered suspicious.

What action the IDS takes when suspicious activity is found depends on what class of intrusion detection system we are talking about. There are two major classes of intrusion detection systems:

- **Passive IDS:** A passive IDS logs suspicious activity to a file and could send an alert to the administrator if alerts have been configured. A passive IDS is normally referred to as just an *IDS*.
- **Active IDS:** An active IDS logs the suspicious activity, sends an alert to the administrator, and also takes corrective action such as preventing the system that is creating the suspicious activity from further accessing the network.

  An active IDS is now known as an *intrusion prevention system* (IPS).

For the CCENT exam, ensure that you are familiar with the purpose of an intrusion detection system. Also, know the difference between an IDS and an IPS.

Switches

I know we talk about switches in detail within Book III, Chapters 3 and 4, but I want to make sure that I mention switches here as a security device because switches have some great features that help protect a network environment. The following are some security features to remember about a switch:

- **Filtered traffic:** The purpose of a switch is to filter traffic by sending the traffic to only the port where the destination MAC address of the frame is connected to the switch. This aids in security, as someone else connected to the switch cannot easily run a packet sniffer and see all traffic on the network. Because the traffic is not sent to the port of the person doing the sniffing, there is no opportunity for that person to capture and view network traffic.
- **Port security:** Port security is the feature on a switch that allows you to limit which systems can connect to which ports on the switch. With port security, you associate the MAC address of a system with the port, and no other system can connect to that port.

- **Disable ports:** For security reasons, you need to disable any ports on the switch that you are not using. This prevents someone from connecting an unknown system to the network without your knowledge.
- **VLANs:** Virtual LANs allow you to create communication boundaries on the switch. You can create multiple VLANs on the switch and then place different ports into different VLANs. Systems that are connected to ports in one VLAN cannot communicate with systems in another VLAN without the use of a router.

You find out how to configure security features of Cisco switches in the next chapter.

Virtual Private Networks

The final security technology I want to mention is what is known as a *virtual private network,* or VPN. A VPN is responsible for creating an encrypted tunnel across an unsecure network such as the Internet. Once the tunnel is created between the client and the VPN server, any data that is sent through the tunnel is encrypted.

Looking at Figure 1-6, you see that you are in a hotel room in Toronto and want to access some files that are in your office in New York. Normally, you would not try to access those files across the Internet because you would not want the information sent or received in plain text for someone to intercept.

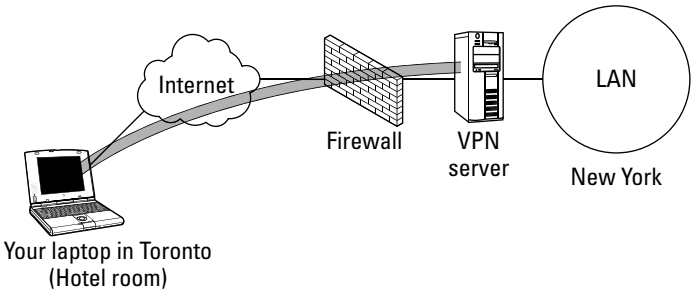

Figure 1-6: A VPN creates an encrypted tunnel over an unsecure network so that data can be sent and received securely.

As a solution, you install VPN client software on your laptop, which connects across the Internet to the VPN server in New York. After the VPN server authenticates you with your username and password, you are granted access to the network, and the encrypted tunnel is created. Now any data sent between the VPN client and the VPN server is secure, as it is encrypted in transit.

VPN protocols are responsible for encrypting the data. Examples of VPN protocols are the Point-to-Point Tunneling Protocol (PPTP) and the Layer 2 Tunneling Protocol (L2TP). Growing in popularity is SSL VPNs, which do not require VPN client software on the client systems as the Web browser makes the client connection. It should also be noted that VPNs can be created from one site to another in order to encrypt all traffic between the two sites (as opposed to the clients creating the VPN).

Mitigating Security Threats

Now that you have been introduced to some of the different types of network attacks and identified some of the popular network security appliances, let's take a look at how you can minimize potential network threats. A fancy term for minimizing the threats is *mitigating*.

Although this section is not intended to be a complete list of the steps to take to secure your environment, it is definitely a list of some of the fundamental steps you should take — and they will go a long way to helping create a secure environment.

Workstations

To help keep your desktop workstations secure, you should consider doing the following, at a minimum:

- **Patch your systems.** Be sure to keep your systems up to date with patches. This includes patching the operating system and all software installed.
- **Use antivirus software.** Ensure that you have company-approved antivirus software installed on all desktop systems.
- **Keep virus definitions up to date.** Make sure you are keeping the virus software definitions up to date. These definitions allow the virus-protection software to know what the current viruses are.
- **Limit administrative accounts.** Do not give all the users administrative capabilities to the desktop system. Ensure that most users utilize restricted accounts and limit how many people have administrative access.
- **Maintain user awareness.** It is important to ensure users are aware of some of the different threats that exist. Educate users on good e-mail practices and about social engineering attacks.

Servers

To help keep your servers secure you should contemplate doing the following, at a minimum:

- **Patch systems.** Be sure to keep your servers up-to-date with patches. This includes patching the operating system and all software installed.
- **Use server-class antivirus software.** Ensure that you have company-approved antivirus software that is designed to run on servers.
- **Keep virus definitions up-to-date.** Make sure that you are keeping the virus software definitions up-to-date. These definitions allow the virus-protection software to know what the current viruses are.
- **Limit administrative accounts.** Ensure that you limit how many people have administrative access to the servers. The more people making changes to a server, the more chances mistakes will happen.
- **Configure permissions.** Make certain that all the resources are secured with appropriate permissions.
- **Place server in a secure room.** Be sure that servers are placed in a locked server room, where access to that room is limited to authorized personnel.
- **Install a firewall.** Depending on the type of server, you may decide to limit what traffic can reach the server by installing a software firewall on the system. For example, if the system is used only as a Web server, I recommend installing a software firewall that allows only HTTP and HTTPS traffic to the system.

Network

To help create a more secure network environment, you should consider following these general steps, at a minimum:

- **Encrypt traffic.** Depending on how sensitive the information is that travels on your network, you may decide to encrypt all network traffic.
- **Use firewalls.** Use firewalls to control what type of traffic is allowed to enter and leave different areas of the network.
- **Use intrusion detection systems.** Be sure to configure an IDS or IPS to monitor network activity and notify you of any suspicious activity.
- **Place switches and routers in a secure room.** Make sure you are storing switches and routers in a locked server room where you are limiting access to the room.
- **Implement device security best practices.** Ensure that on your switches and routers you are following security best practices such as configuring passwords, encrypting passwords, and using other switch and router device security concepts mentioned in the next chapter!

Chapter Summary

This chapter covers the fundamental concepts regarding network security. It is an important topic, but understand that this chapter only scratches the surface of security concepts. For the CCENT certification, be familiar with the following facts about security:

- *Authentication* is proving your identity to the system.
- *Authorization* is granting someone access to a system or resource after he has been authenticated.
- *CIA* stands for confidentiality, integrity, and availability.
- A *social engineering attack* is when the hacker tries to trick someone into compromising security through an e-mail or phone call.
- A *buffer overflow attack* is when the hacker sends too much data to an application, which normally results in administrative control of the system in a command shell.
- There are three types of password attacks: dictionary, hybrid, and brute force.
- A *denial of service* (DoS) attack is when a hacker attacks a system or device by overloading it and causing it to crash or be too busy to perform its job.
- *Firewalls* control what traffic can enter the network.
- An *intrusion detection system* detects suspicious activity and alerts the administrator.
- A *VPN* creates an encrypted tunnel over an unsecure network such as the Internet.

Lab Exercises

This chapter introduces you to the world of security by exposing you to some popular security terms and attack types. The following labs help you review the security concepts discussed in this chapter.

Lab 1-1: Security terminology

In this lab, review basic security terms by matching the term with the appropriate description.

Term	Description
___ Vulnerability	**A.** Verifying a user's identity.
___ Packet-filtering firewall	**B.** Creates an encrypted tunnel over an unsecure network.
___ Authentication	**C.** Filters traffic by understanding the context of the conversation.
____Mitigating threats	**D.** A weakness in a piece of software or hardware.
___ CIA	**E.** An area of the network used to place servers that are accessed from the Internet.
___ VPN	**F.** Implementing security controls to minimize the threats against a system or device.
___ DMZ	**G.** A device that identifies suspicious activity on a system or network.
___ Stateful packet inspection firewall	**H.** The fundamental goals of information security.
___ IDS	**I.** Inspects the fields in the header of the packet to decide whether to allow or deny the traffic.

Lab 1-2: Types of attacks

In this lab, review the different types of attacks by matching the term with the appropriate description.

Term	Description
___ Denial of service	**A.** Type of malicious software that the user is tricked into installing; it allows the hacker access to the system.
___ IP spoofing	**B.** Capturing network packets and being able to view information in the packets.
___ Buffer overflow	**C.** Overloading a system, which results in the system not being able to perform its job.
___ Eavesdrop attack	**D.** A type of password attack that tries dictionary words but also adds numbers to the end of each word.
___ Social engineering attack	**E.** A self-replicating virus.
___ MAC spoofing	**F.** Sending too much data input to an application.
___ Trojan virus	**G.** Altering the layer-3 source address of a packet.
___ Hybrid attack	**H.** Altering the layer-2 source address of a packet.
___ Worm virus	**I.** A hacker tries to trick you into compromising security through social contact.

Prep Test

1 **What type of firewall can allow or deny traffic after inspecting the application data in the packet?**

A ❍ Application-level firewall
B ❍ Stateful packet inspection firewall
C ❍ Personal firewall
D ❍ Packet-filtering firewall

2 **Which of the following is a form of denial of service attack? (Select all that apply.)**

A ❑ SYN flood
B ❑ Spoof attack
C ❑ Brute force attack
D ❑ Ping of death

3 **What is the term used for the area of the network where you are to place servers from the Internet?**

A ❍ IDS
B ❍ Private LAN
C ❍ DMZ
D ❍ Internal LAN

4 **What type of attack involves the hacker contacting the victim through e-mail or a phone call?**

A ❍ Social engineering attack
B ❍ Denial of service
C ❍ E-mail attack
D ❍ Contact attack

5 **What type of firewall is capable of inspecting the fields found *only* in the header of the packet?**

A ❍ Application-level firewall
B ❍ Stateful packet inspection firewall
C ❍ Windows firewall
D ❍ Packet-filtering firewall

6 **What type of attack involves the hacker sending too much data to the application, which normally results in administrative access within a command shell?**

A ❍ Spoof attack
B ❍ Buffer overflow attack
C ❍ Social engineering attack
D ❍ Denial of service attack

7 **What type of attack involves the hacker modifying the source IP address of a packet in order to try to bypass the security control?**

A ❍ Spoof attack
B ❍ Buffer overflow attack
C ❍ Social engineering attack
D ❍ Denial of service attack

8 **What type of password attack mathematically calculates all possible password combinations?**

A ❍ Dictionary
B ❍ Hybrid
C ❍ Brute force
D ❍ Calculated

9 **What type of firewall knows about the context of the conversation and whether the packet is the right packet at that point in time?**

A ❍ Spoof firewall
B ❍ Stateful packet inspection firewall
C ❍ Screened firewall
D ❍ Packet-filtering firewall

10 **Which of the following take corrective action when suspicious activity is detected? (Select two.)**

A ❑ Active IDS
B ❑ Passive IDS
C ❑ IPS
D ❑ NAT

Answers

1. **A.** Application-level firewalls can inspect the application-level data, such as what application command is executing, and either allow or deny that traffic. *See "Firewalls."*
2. **A, D.** A SYN flood attack and the ping of death attack were popular denial of service attacks years back. *Review "Denial of service."*
3. **C.** The demilitarized zone (DMZ) is where you should place public servers such as Web and DNS servers. *Check out "Firewalls."*
4. **A.** A social engineering attack is when the hacker contacts the victim and tries to trick the individual into compromising security. *Peruse "Social engineering attacks."*
5. **D.** A packet-filtering firewall is capable of inspecting only the packet header to decide if the packet should be allowed or denied. This type of firewall could be easily tricked with a spoof attack. *Take a look at "Firewalls."*
6. **B.** A buffer overflow attack involves the hacker sending too much data to the application, which typically results in administrative access to the system. *Peek at "Buffer overflow."*
7. **A.** A spoof attack is when the hacker alters the source address of a packet in order to bypass a security control such as a firewall or access control list. *Look over "Spoofing."*
8. **C.** A brute force attack mathematically calculates all potential password combinations. *Study "Password attacks."*
9. **B.** A stateful packet inspection firewall knows the context of the conversation and the order in which packets should be received. For example, the firewall knows that you can send data to a Web server without a three-way handshake. *Refer to "Firewalls."*
10. **A, C.** An active IDS takes corrective action when suspicious activity is detected. Active IDSes are now known as intrusion prevention systems (IPS). *Examine "Intrusion detection system."*